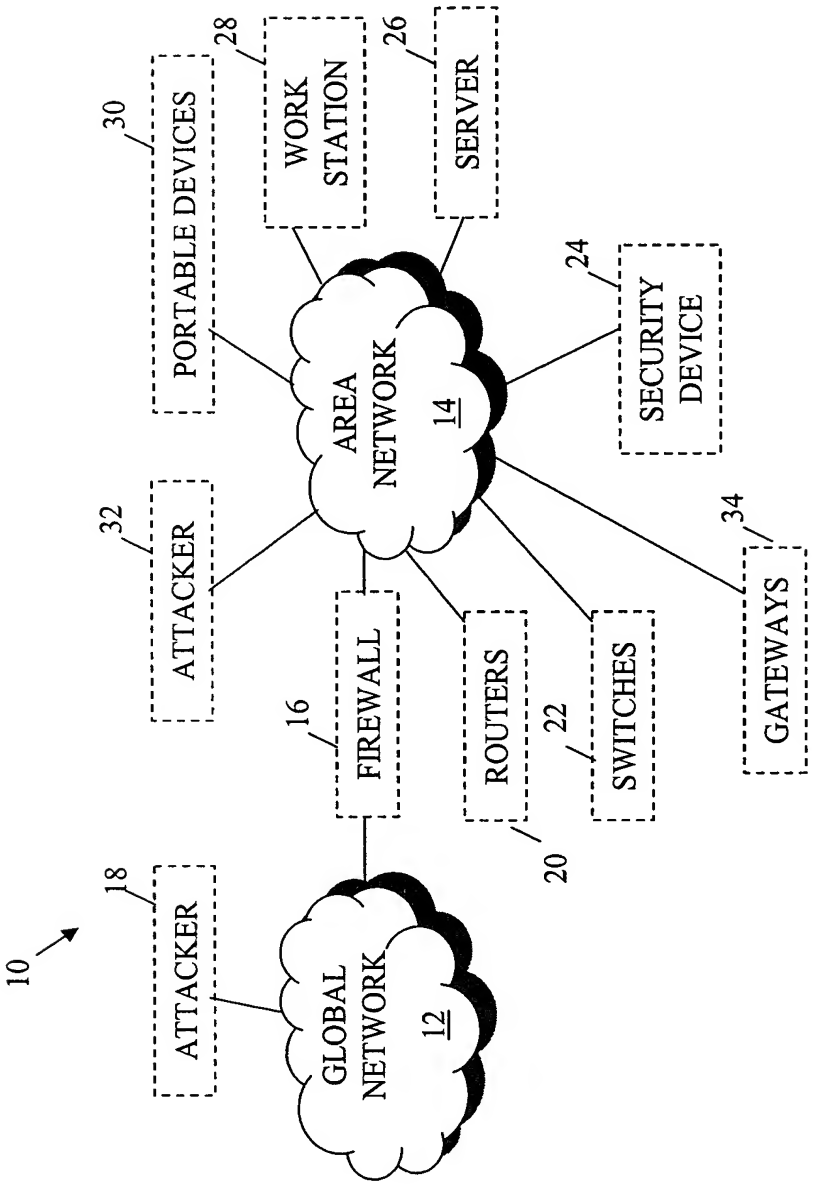
10
GLOBAL NETWORK 12
AREA NETWORK 14
FIREWALL 16
ATTACKER 18
ROUTERS 20
SWITCHES 22
SECURITY DEVICE 24
SERVER 26
WORK STATION 28
PORTABLE DEVICES 30
ATTACKER 32
GATEWAYS 34

FIGURE 1

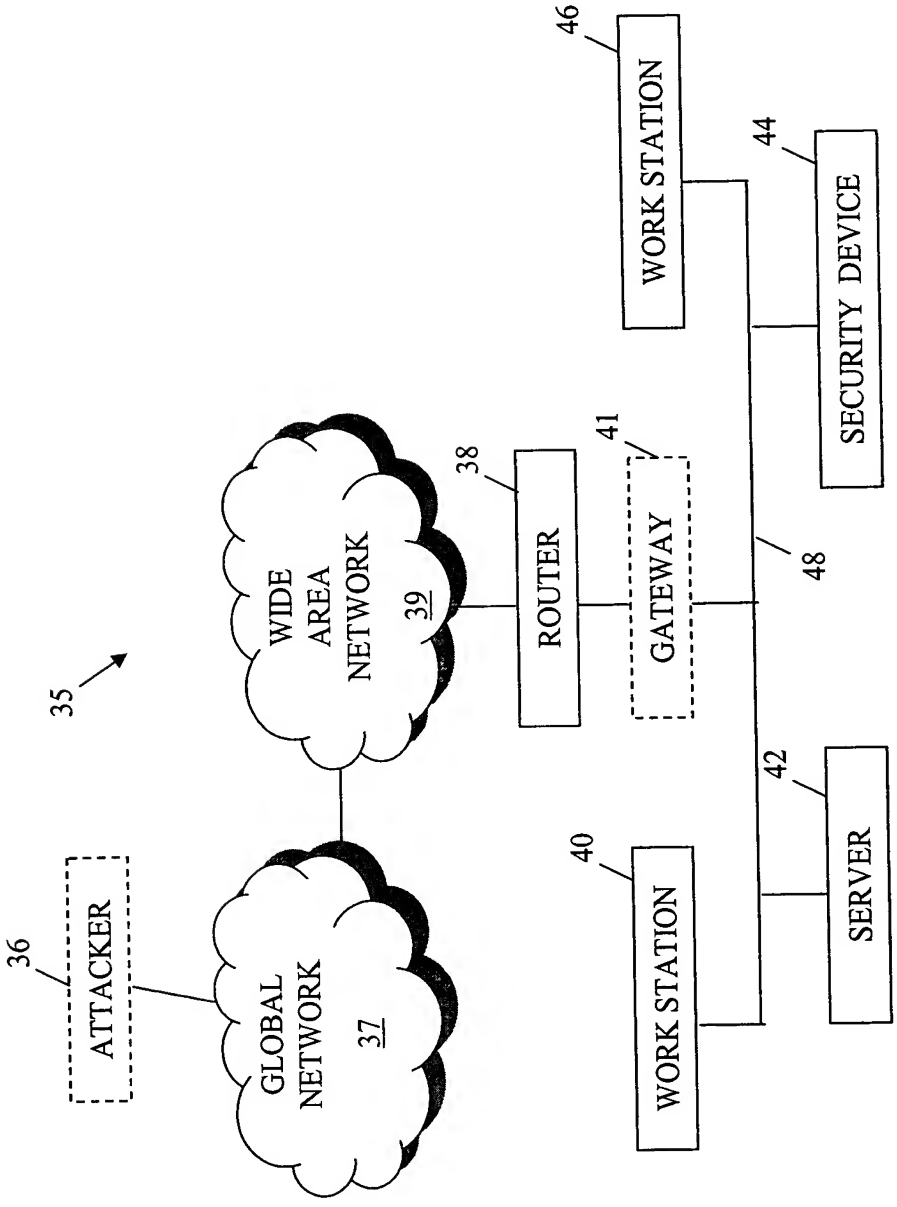
35
36
ATTACKER
GLOBAL NETWORK 37
WIDE AREA NETWORK 39
38
ROUTER
41
GATEWAY
46
WORK STATION
44
SECURITY DEVICE
48
40
WORK STATION
42
SERVER

FIGURE 2

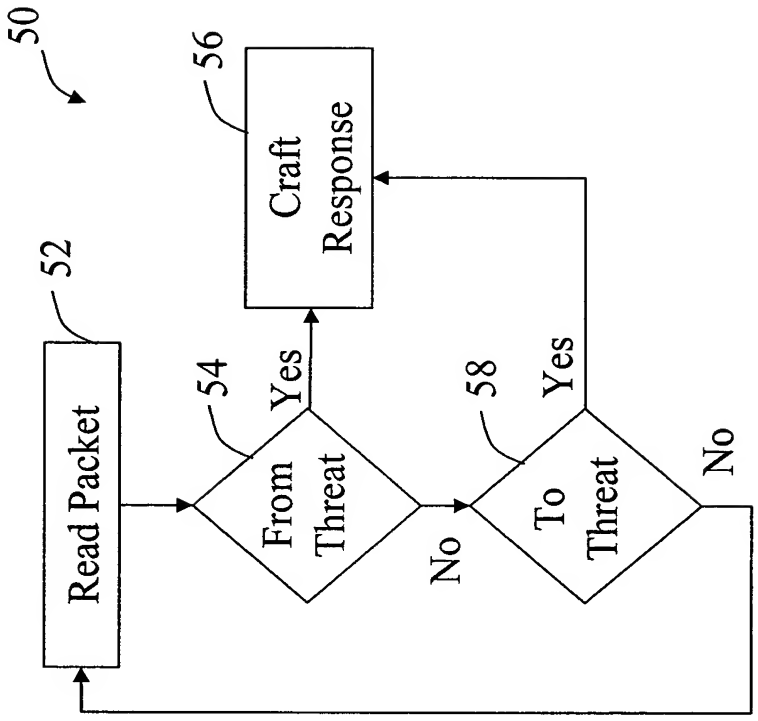
50
52
Read Packet
54
From Threat
Yes
56
Craft Response
No
58
To Threat
Yes
No

FIGURE 3

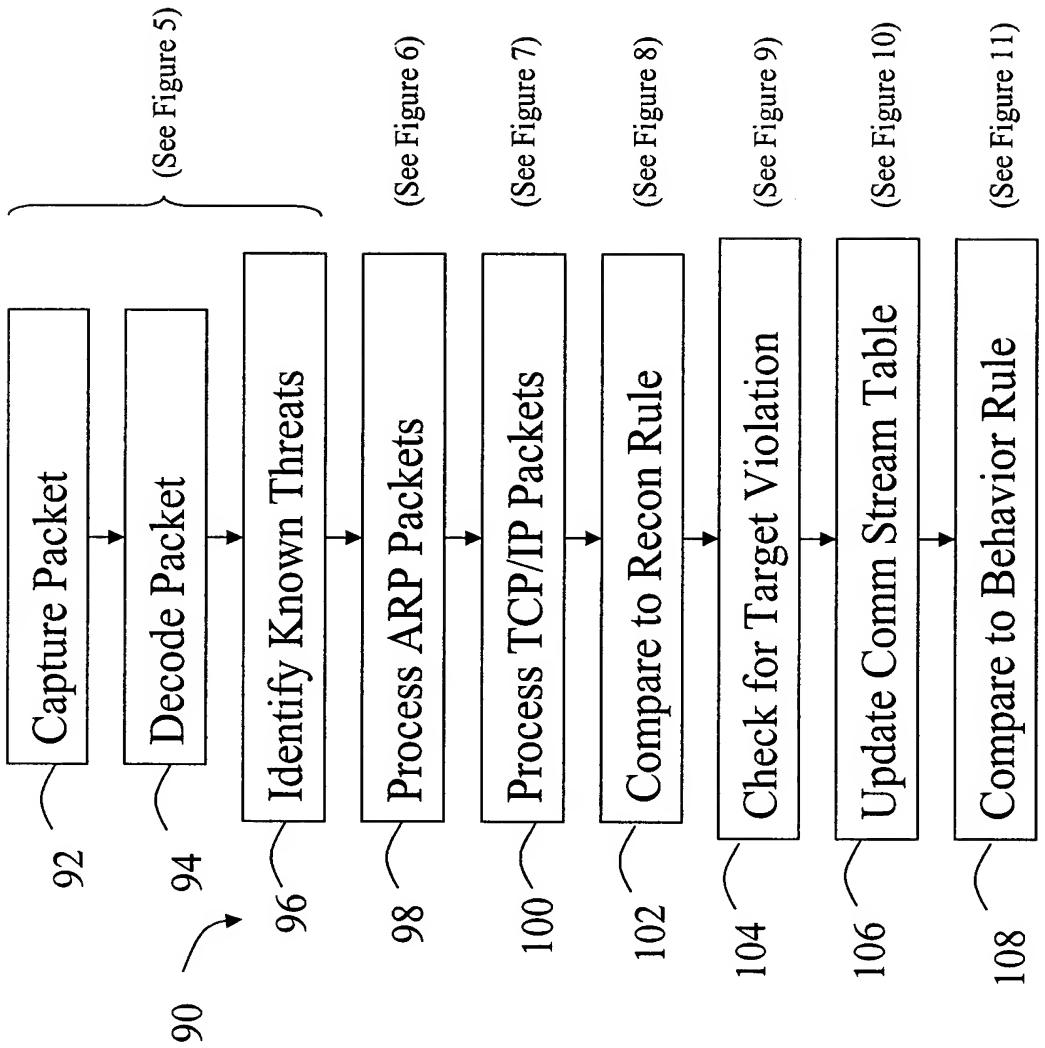
Capture Packet
Decode Packet
Identify Known Threats
Process ARP Packets
Process TCP/IP Packets
Compare to Recon Rule
Check for Target Violation
Update Comm Stream Table
Compare to Behavior Rule
(See Figure 5)
(See Figure 6)
(See Figure 7)
(See Figure 8)
(See Figure 9)
(See Figure 10)
(See Figure 11)
90
92
94
96
98
100
102
104
106
108

FIGURE 4

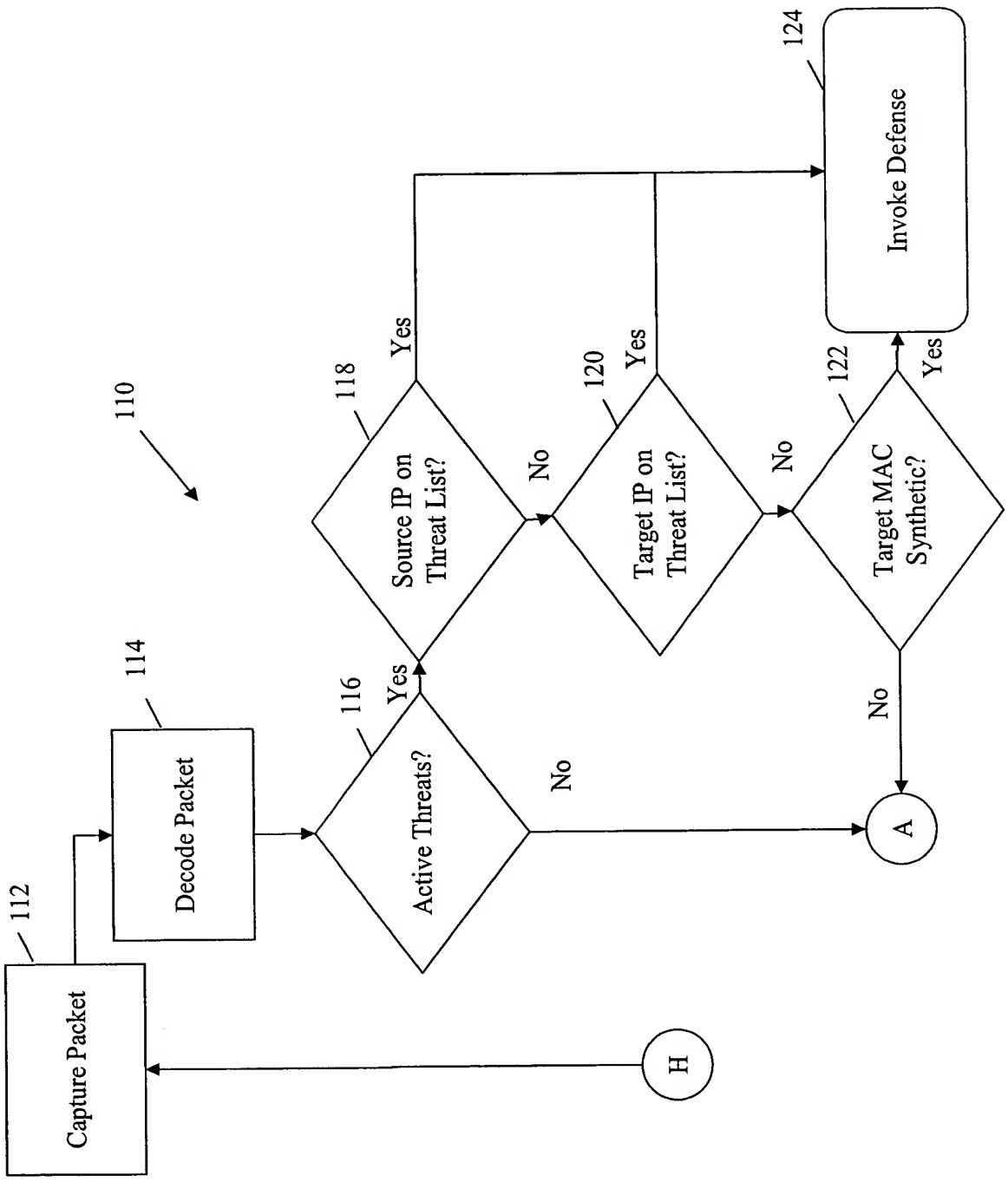
110
112
Capture Packet
114
Decode Packet
116
Active Threats?
Yes
No
118
Source IP on Threat List?
Yes
No
120
Target IP on Threat List?
Yes
No
122
Target MAC Synthetic?
Yes
No
124
Invoke Defense
H
A

FIGURE 5

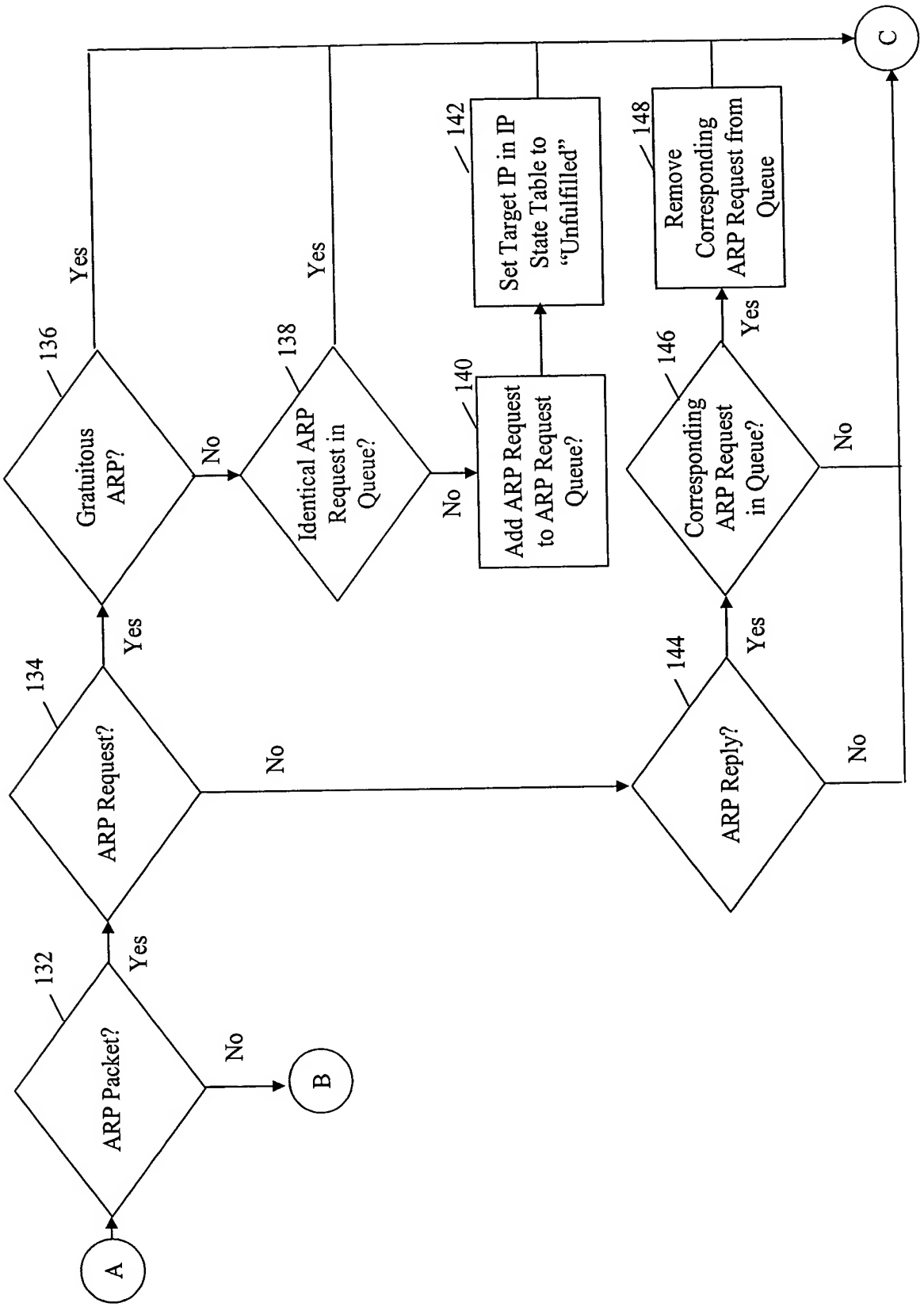
A
ARP Packet?
132
Yes
No
B
ARP Request?
134
Yes
No
Gratuitous ARP?
136
Yes
No
Identical ARP Request in Queue?
138
Yes
No
Add ARP Request to ARP Request Queue?
140
Set Target IP in IP State Table to "Unfulfilled"
142
ARP Reply?
144
Yes
No
Corresponding ARP Request in Queue?
146
Yes
No
Remove Corresponding ARP Request from Queue
148
C

FIGURE 6

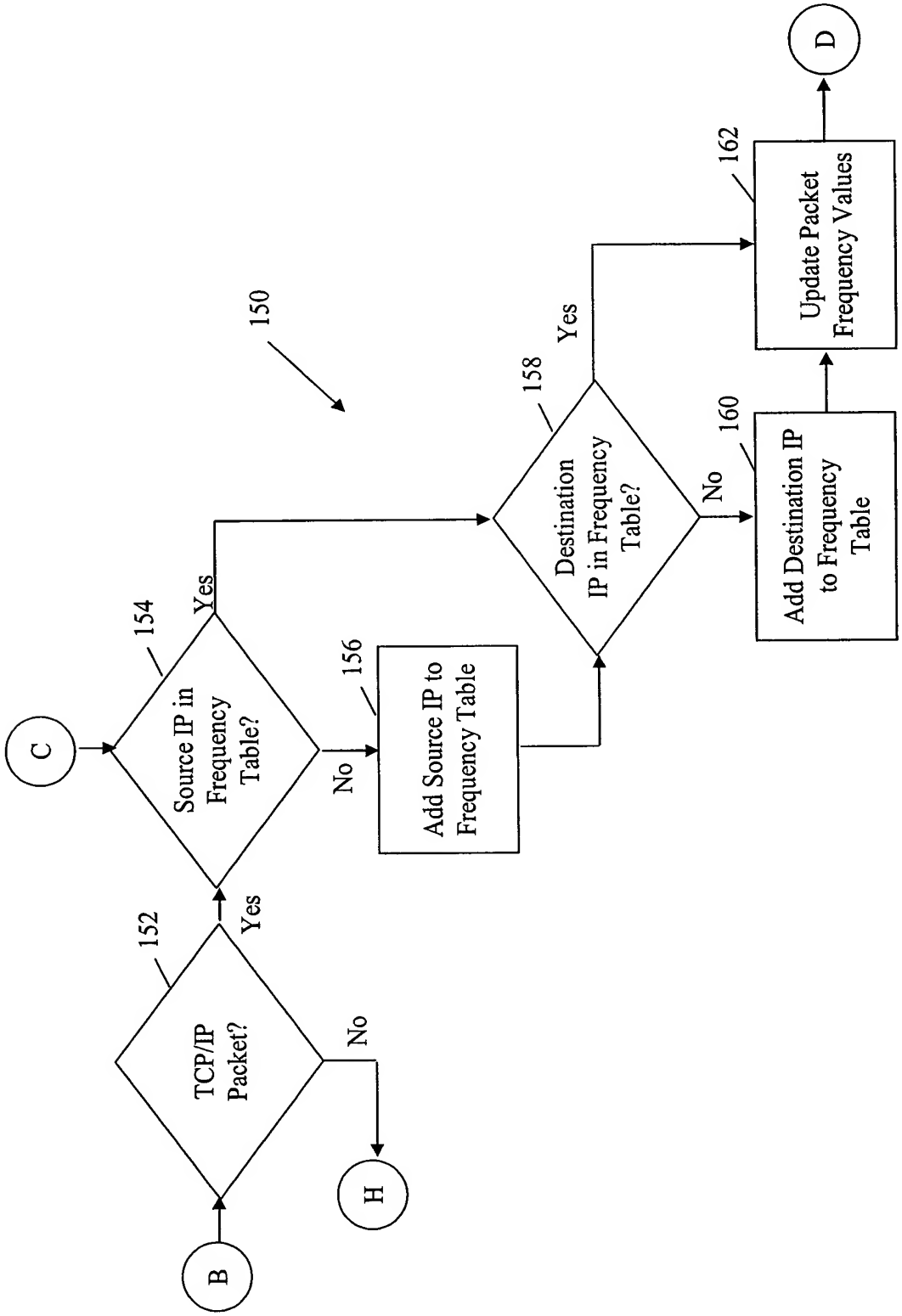
150
B
TCP/IP Packet?
152
Yes
No
H
C
Source IP in Frequency Table?
154
Yes
No
Add Source IP to Frequency Table
156
Destination IP in Frequency Table?
158
Yes
No
Add Destination IP to Frequency Table
160
Update Packet Frequency Values
162
D

FIGURE 7

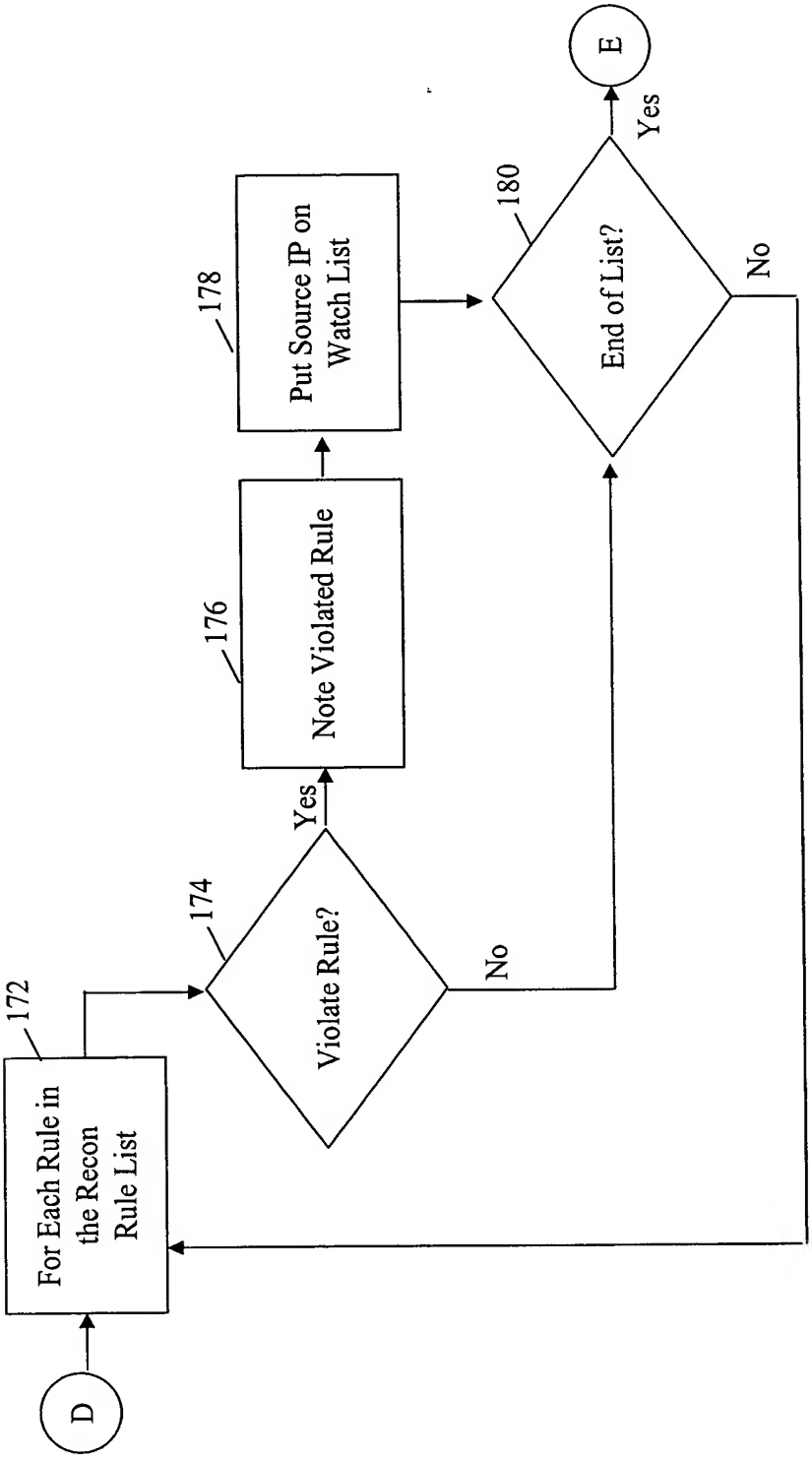
D
For Each Rule in the Recon Rule List
172
Violate Rule?
174
Yes
No
Note Violated Rule
176
Put Source IP on Watch List
178
End of List?
180
Yes
No
E

FIGURE 8

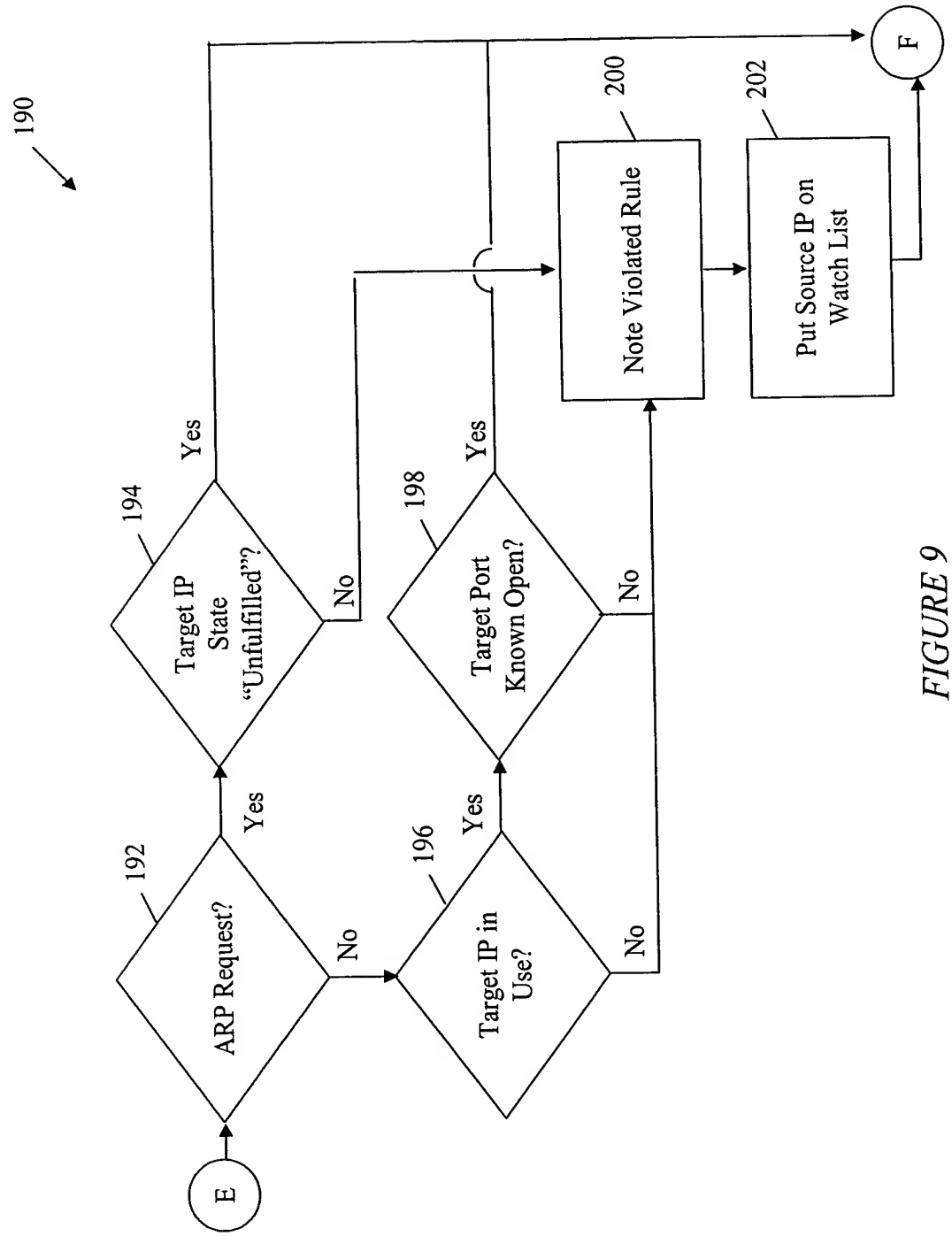
190
E
192
ARP Request?
Yes
No
194
Target IP State "Unfulfilled"?
Yes
No
196
Target IP in Use?
Yes
No
198
Target Port Known Open?
Yes
No
200
Note Violated Rule
202
Put Source IP on Watch List
F

FIGURE 9

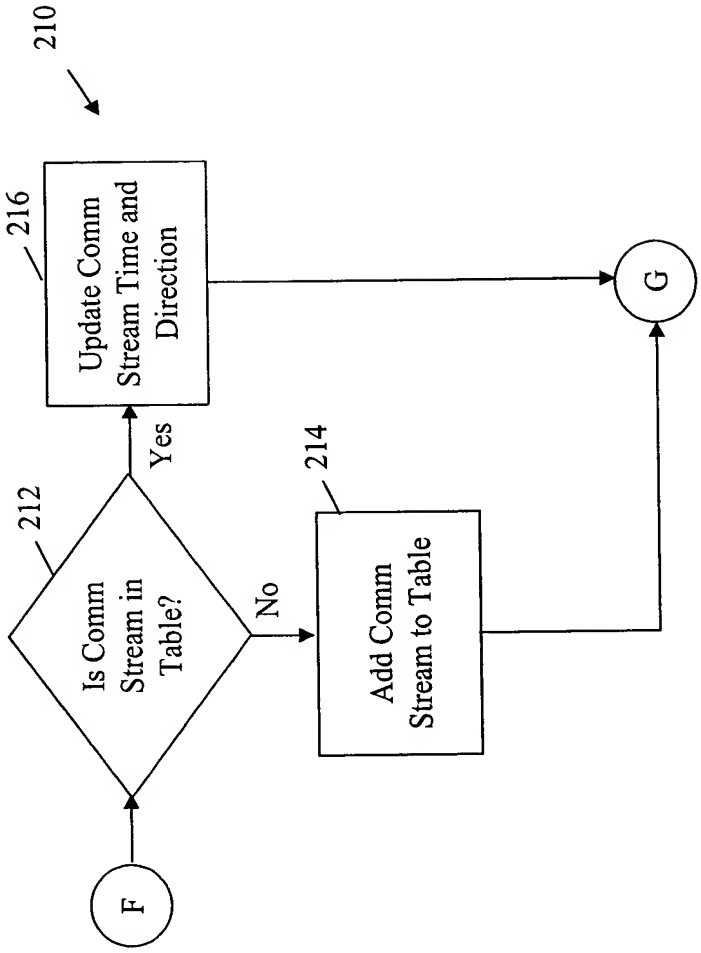
210
216
Update Comm Stream Time and Direction
G
Yes
214
212
Is Comm Stream in Table?
No
Add Comm Stream to Table
F

FIGURE 10

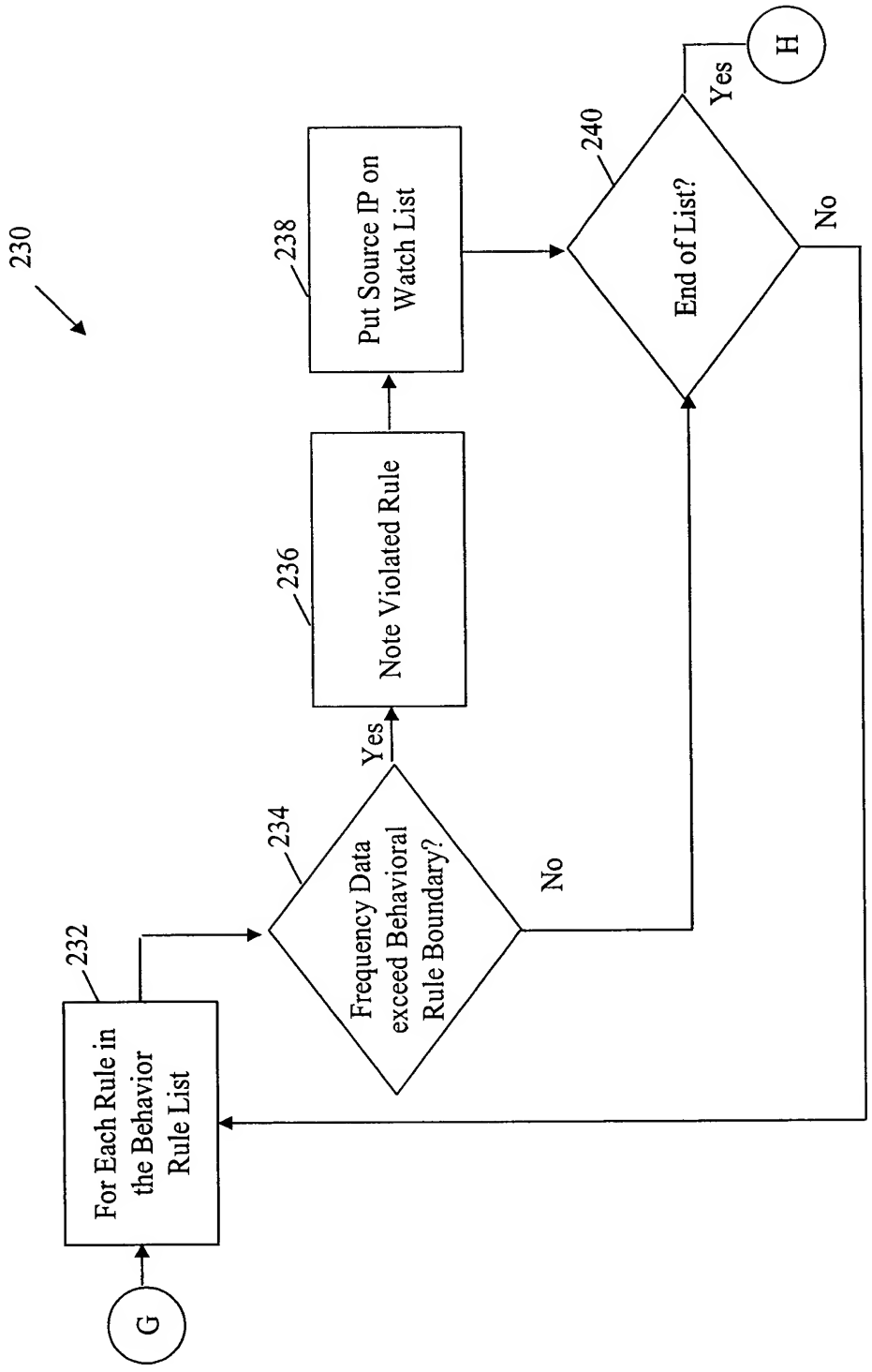
230
G
For Each Rule in the Behavior Rule List
232
Frequency Data exceed Behavioral Rule Boundary?
234
Yes
No
Note Violated Rule
236
Put Source IP on Watch List
238
End of List?
240
Yes
No
H

FIGURE 11

SIP	DIP	SMAC	TIME
183.76.0.7	192.82.0.1	00-08-21-C9-3e-CO	00:00:00.000

FIGURE 12

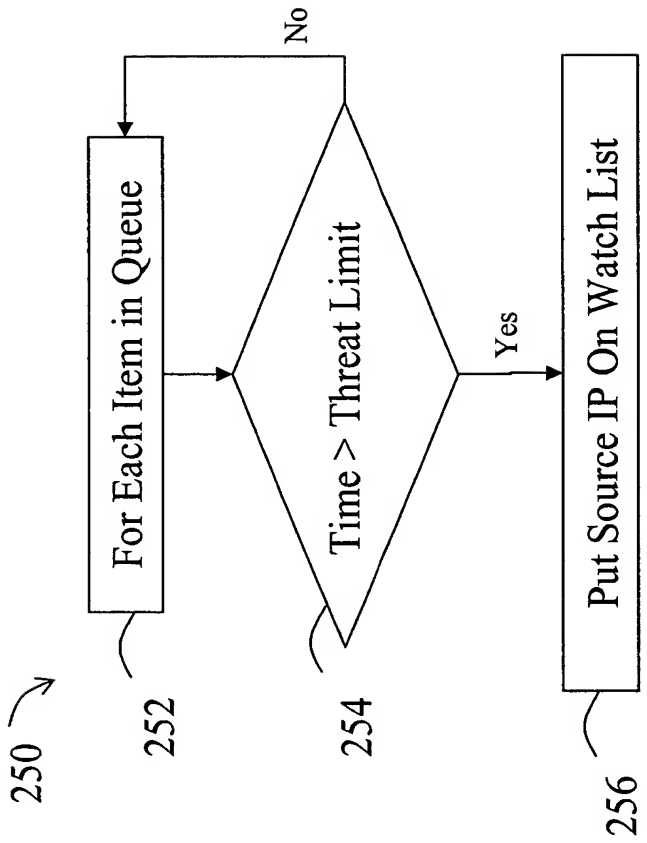

FIGURE 13

SIP	DIP	SMAC	TIME	RULE
183.76.0.7	192.82.0.1	00-08-21-C9-3e-C0	00:00:00.000	5

FIGURE 14

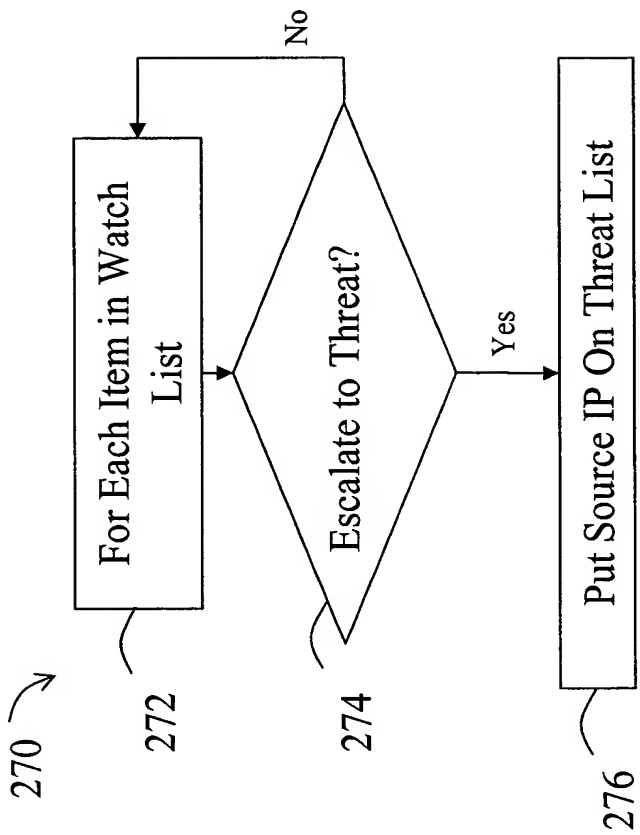

FIGURE 15

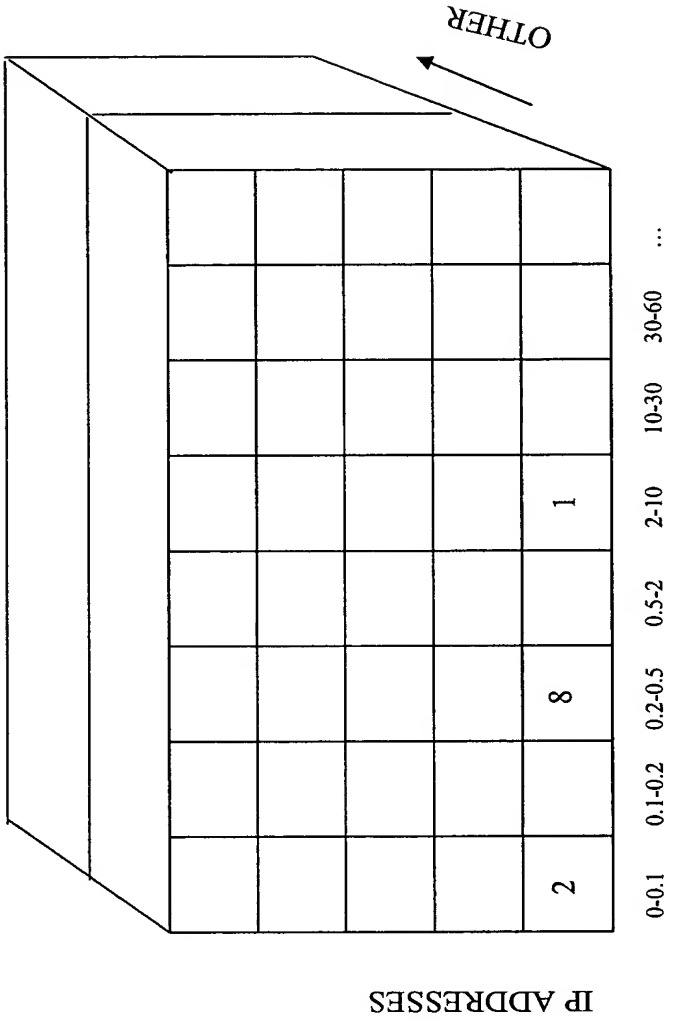

FIGURE 16

IP	STATE
192.82.0.1	1
192.82.0.2	4
183.76.0.7	3

FIGURE 17

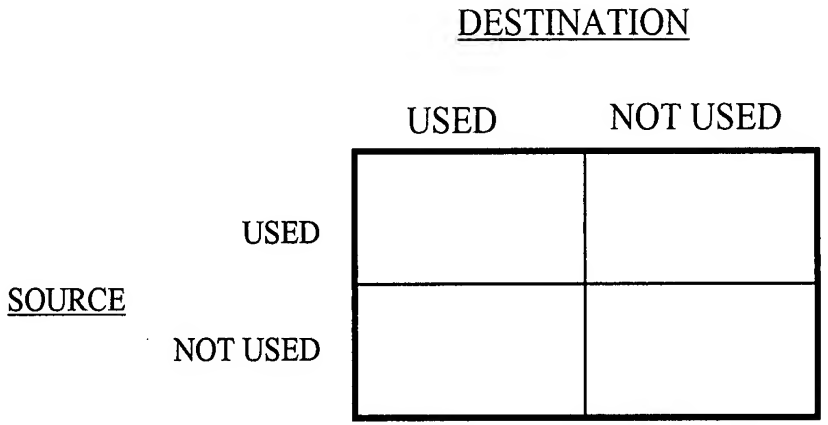

FIGURE 18

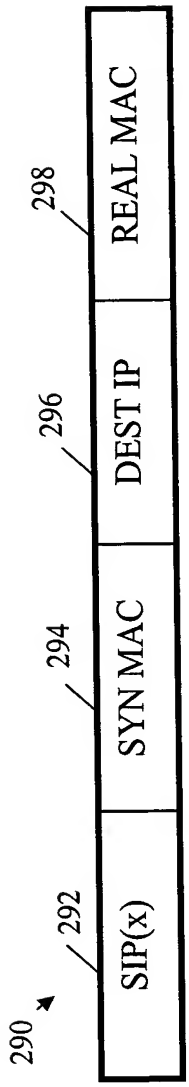

FIGURE 19

IP1	IP2	No.	Dir.	Time
183.76.0.7	192.82.0.1	10	1	00:00:00.000

FIGURE 20

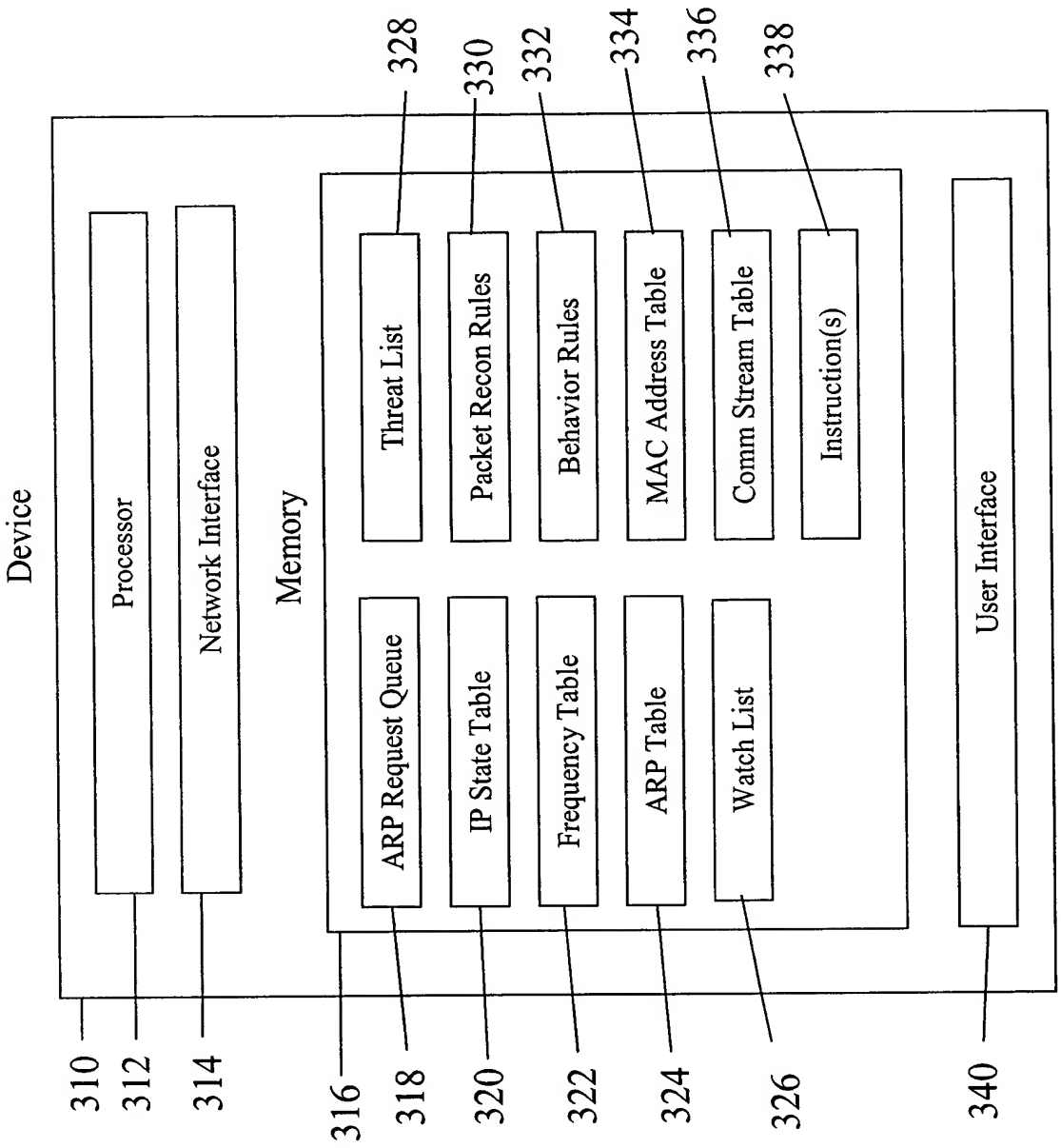
Device
Processor
Network Interface
Memory
Threat List
Packet Recon Rules
Behavior Rules
MAC Address Table
Comm Stream Table
Instruction(s)
ARP Request Queue
IP State Table
Frequency Table
ARP Table
Watch List
User Interface
310
312
314
316
318
320
322
324
326
328
330
332
334
336
338
340

FIGURE 21

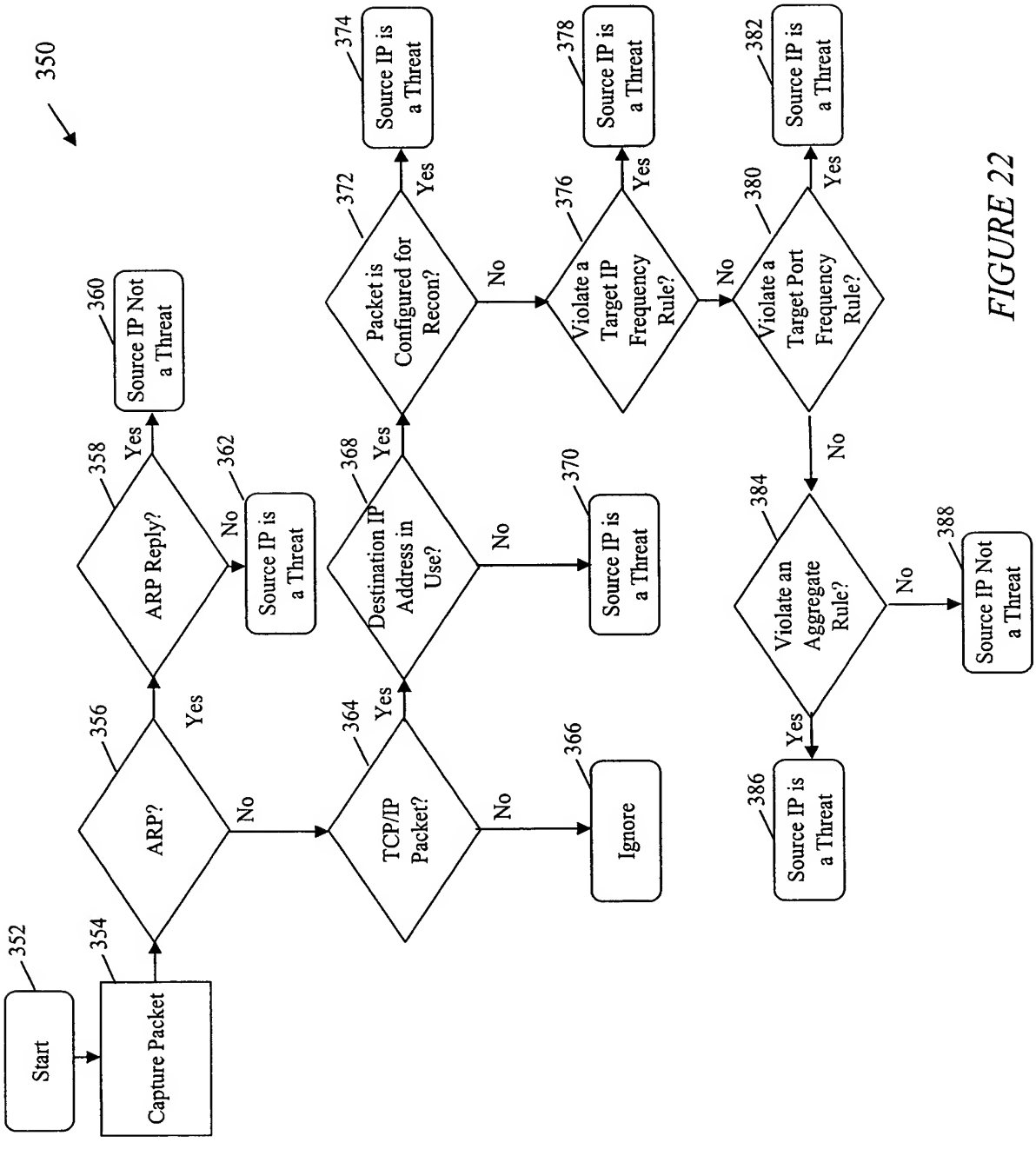
350
Start
352
Capture Packet
354
ARP?
356
Yes
No
ARP Reply?
358
Yes
No
Source IP Not a Threat
360
Source IP is a Threat
362
TCP/IP Packet?
364
Yes
No
Ignore
366
Destination IP Address in Use?
368
Yes
No
Source IP is a Threat
370
Packet is Configured for Recon?
372
Yes
No
Source IP is a Threat
374
Violate a Target IP Frequency Rule?
376
Yes
No
Source IP is a Threat
378
Violate a Target Port Frequency Rule?
380
Yes
No
Source IP is a Threat
382
Violate an Aggregate Rule?
384
Yes
No
Source IP is a Threat
386
Source IP Not a Threat
388

FIGURE 22

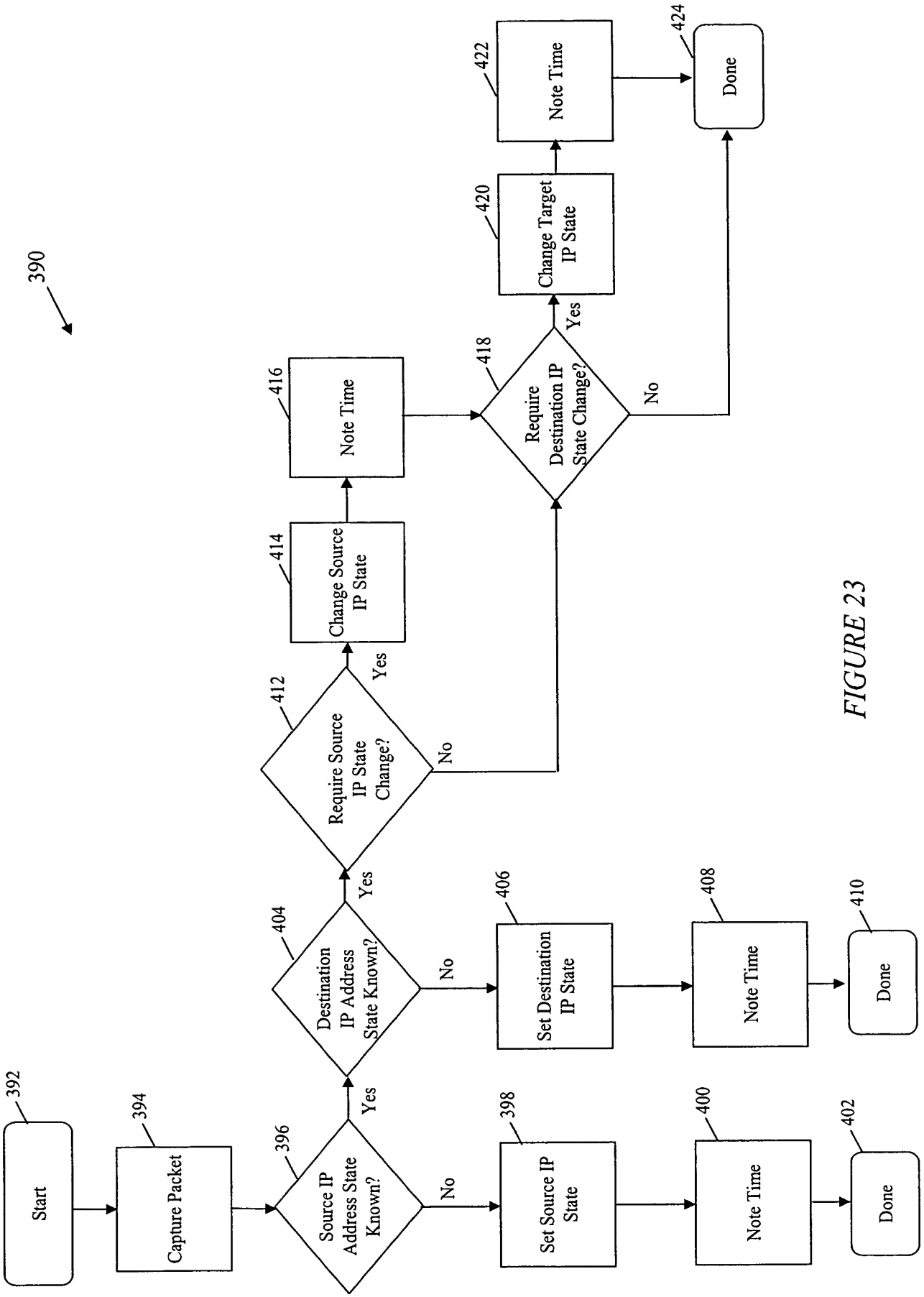
390
Start
392
Capture Packet
394
Source IP Address State Known?
396
Yes
No
Set Source IP State
398
Note Time
400
Done
402
Destination IP Address State Known?
404
Yes
No
Set Destination IP State
406
Note Time
408
Done
410
Require Source IP State Change?
412
Yes
No
Change Source IP State
414
Note Time
416
Require Destination IP State Change?
418
Yes
No
Change Target IP State
420
Note Time
422
Done
424

FIGURE 23

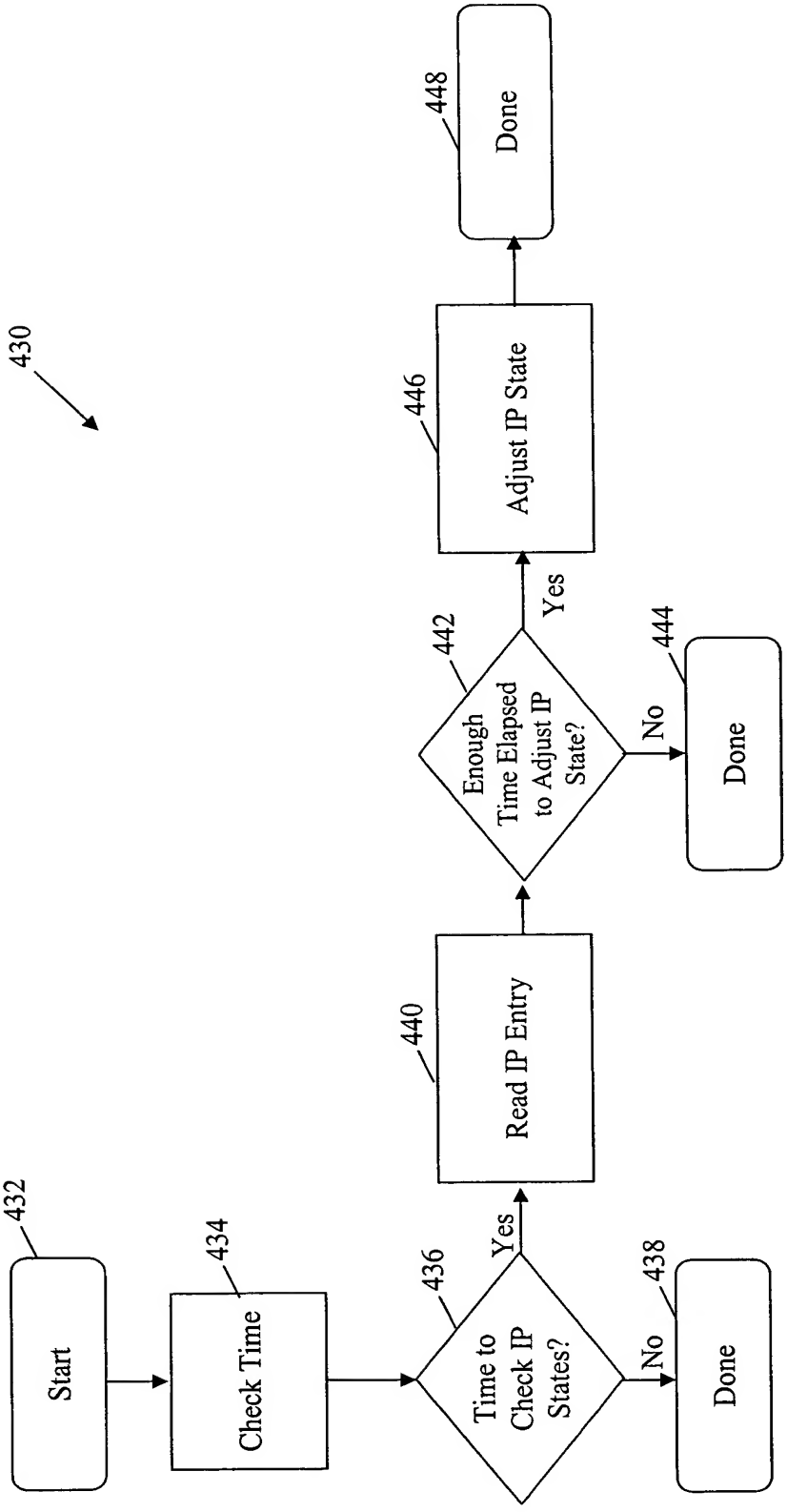
430
432
Start
434
Check Time
436
Time to Check IP States?
Yes
No
438
Done
440
Read IP Entry
442
Enough Time Elapsed to Adjust IP State?
Yes
No
444
Done
446
Adjust IP State
448
Done

FIGURE 24

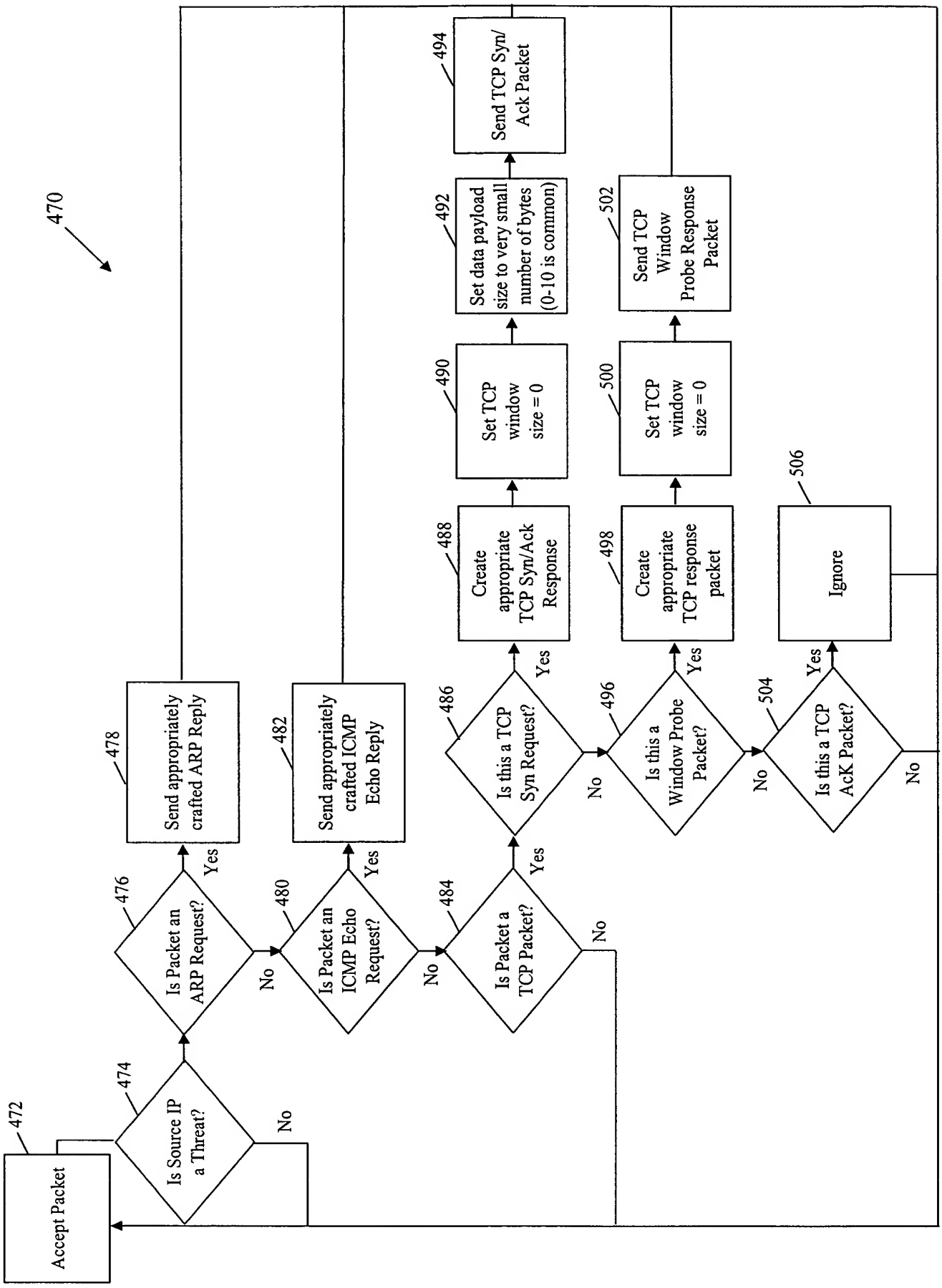
470
Accept Packet
472
Is Source IP a Threat?
474
No
Is Packet an ARP Request?
476
Yes
Send appropriately crafted ARP Reply
478
No
Is Packet an ICMP Echo Request?
480
Yes
Send appropriately crafted ICMP Echo Reply
482
No
Is Packet a TCP Packet?
484
Yes
Is this a TCP Syn Request?
486
Yes
Create appropriate TCP Syn/Ack Response
488
Set TCP window size = 0
490
Set data payload size to very small number of bytes (0-10 is common)
492
Send TCP Syn/ Ack Packet
494
No
Is this a Window Probe Packet?
496
Yes
Create appropriate TCP response packet
498
Set TCP window size = 0
500
Send TCP Window Probe Response Packet
502
No
Is this a TCP AcK Packet?
504
Yes
Ignore
506
No

FIGURE 25

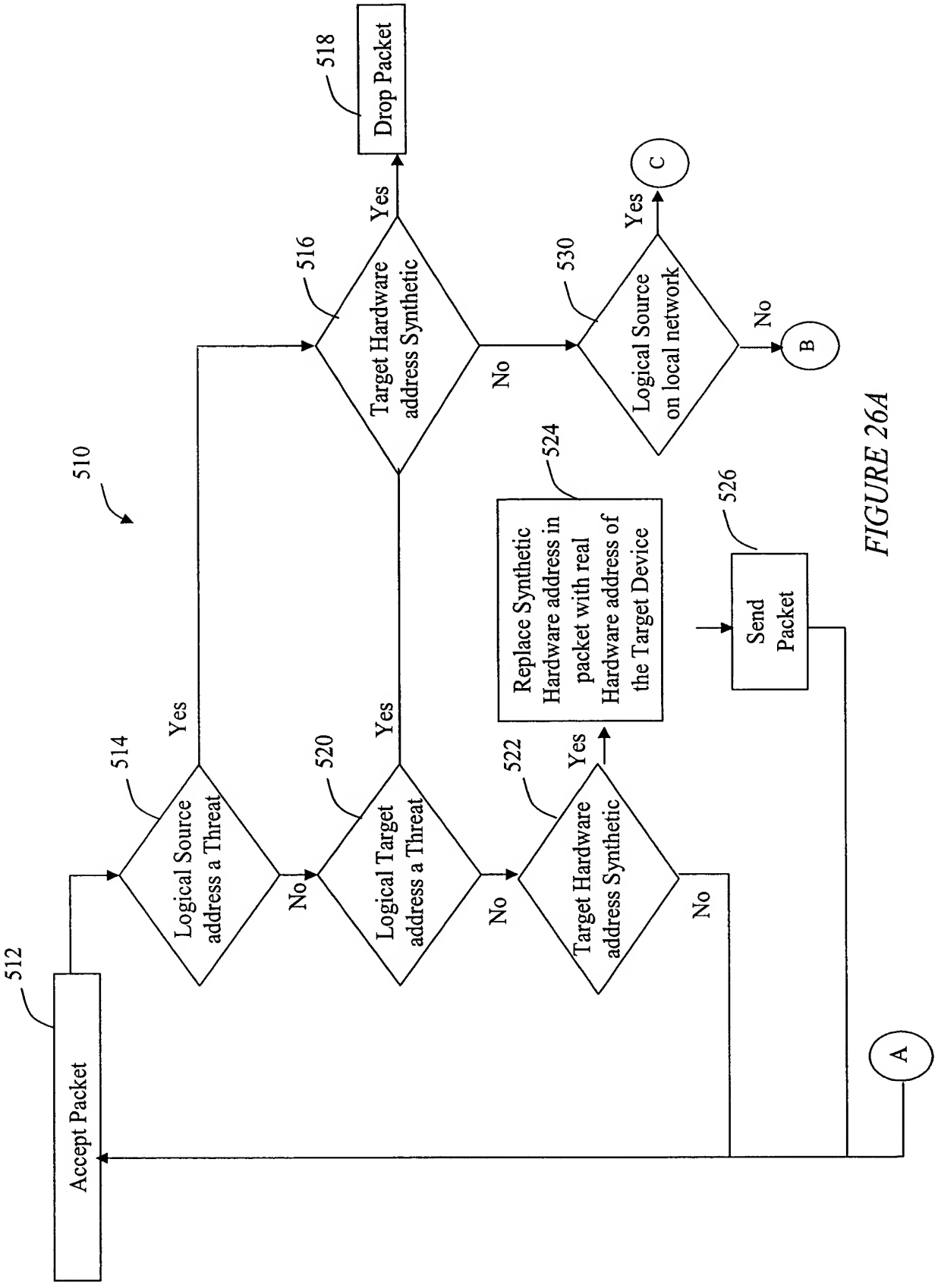
510
512
Accept Packet
514
Logical Source address a Threat
Yes
No
516
Target Hardware address Synthetic
Yes
No
518
Drop Packet
520
Logical Target address a Threat
Yes
No
522
Target Hardware address Synthetic
Yes
No
524
Replace Synthetic Hardware address in packet with real Hardware address of the Target Device
526
Send Packet
530
Logical Source on local network
Yes
No
A
B
C

FIGURE 26A

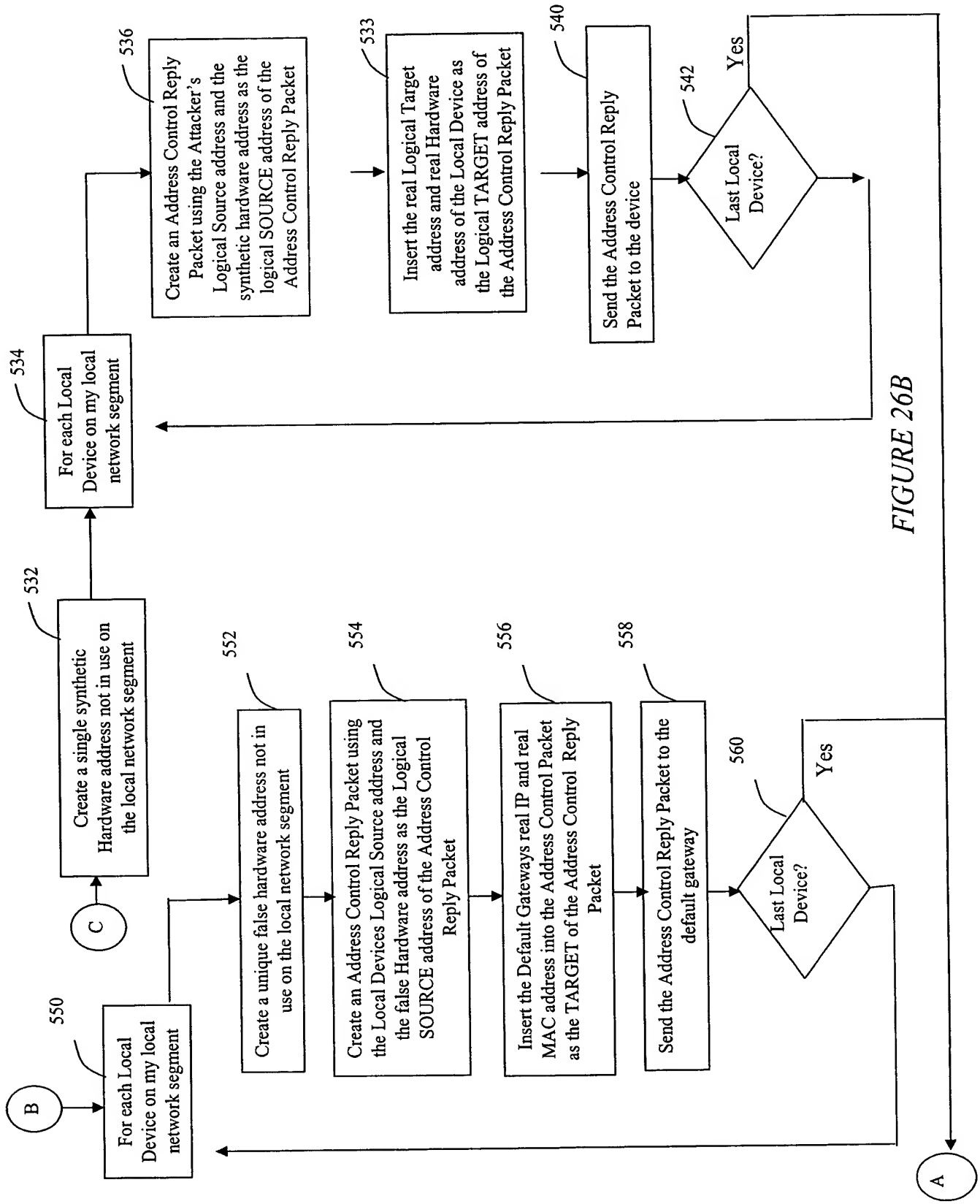
B
550
For each Local Device on my local network segment
C
532
Create a single synthetic Hardware address not in use on the local network segment
534
For each Local Device on my local network segment
552
Create a unique false hardware address not in use on the local network segment
554
Create an Address Control Reply Packet using the Local Devices Logical Source address and the false Hardware address as the Logical SOURCE address of the Address Control Reply Packet
556
Insert the Default Gateways real IP and real MAC address into the Address Control Packet as the TARGET of the Address Control Reply Packet
558
Send the Address Control Reply Packet to the default gateway
560
Last Local Device?
Yes
536
Create an Address Control Reply Packet using the Attacker's Logical Source address and the synthetic hardware address as the logical SOURCE address of the Address Control Reply Packet
533
Insert the real Logical Target address and real Hardware address of the Logical Device as the Logical TARGET address of the Address Control Reply Packet
540
Send the Address Control Reply Packet to the device
542
Last Local Device?
Yes
A

FIGURE 26B

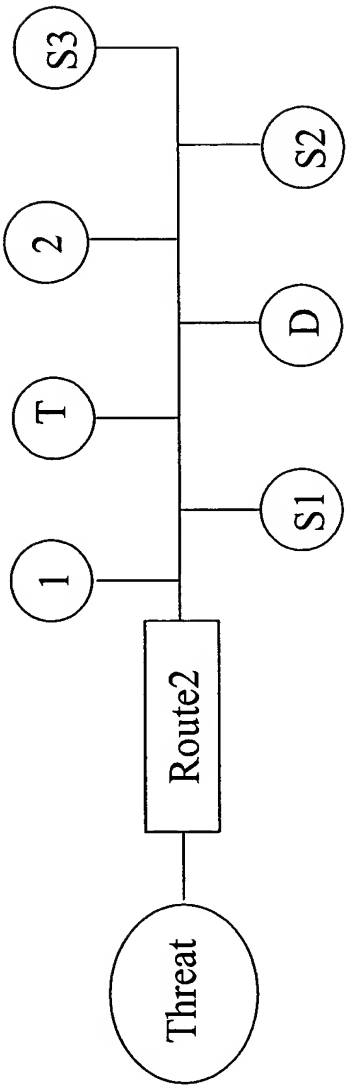

FIGURE 27